

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

JEROLD SHORT and CARLETTE SHORT,
on behalf of themselves and all others
similarly situated,

Plaintiffs,

v.

MR. COOPER GROUP INC.,
Defendant.

Case No.:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Jerold Short and Carlette Short (“Plaintiffs”), individually and on behalf of all others similarly situated, allege the following against Defendant Mr. Cooper Group Inc. (“Defendant” or “Mr. Cooper”), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE CASE

1. Plaintiffs bring this case against Mr. Cooper for its failure to secure and safeguard customers’ personally identifiable information (“PII”)¹ and for failing to provide timely, accurate, and adequate notice to Plaintiffs and Class members that their PII had been compromised.

2. Mr. Cooper is a Texas based loan servicer that “provides servicing, origination and

¹ PII is information that is used to confirm an individual’s identity, and in this instance includes at least an individual’s name, address, email address, phone number, and Social Security number.

transaction-based services related to single family residences throughout the United States.”² Mr. Cooper is one of the largest home loan servicers and originators in the country, currently serving 4.3 million customers.³ Frequently, home buyers are introduced to Mr. Cooper after their mortgage is sold or assigned to the company for servicing.

3. On November 2, 2023, Mr. Cooper posted on its website and filed an 8-K statement announcing that it had sustained a potentially massive data breach in which unauthorized actors gained access to its networks (the “Data Breach”).⁴ While admitting the actors “gained access to certain of our technology systems,” Mr. Cooper failed to disclose which systems were affected, what information was accessed, and how many of its 4.3 million customers were impacted.⁵

4. Mr. Cooper also omitted when the breach began, disclosing only that it discovered the unauthorized access on October 31, 2023. It is unclear from Mr. Cooper’s statements whether the breach has actually been contained.

5. Although Mr. Cooper’s disclosures have been scarce, the available evidence suggests the Data Breach is massive in size and scope. Millions of customers went days without being able to make mortgage payments, and other customers report having experienced

² Mr. Cooper Group, Oct. 2023 Form 10-Q, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/6ea7ec4e-5b61-47c1-b6d8-ba74e4ccd120.pdf> (last visited Nov. 20, 2023).

³ Cyberattack Disrupts Mortgage Payments for Millions of Mr. Cooper Customers, *New York Times* (Nov. 7. 2023), <https://www.nytimes.com/2023/11/07/business/cyberattack-mr-cooper-mortgages.html>.

⁴ Of note, although Mr. Cooper has stated it believes the Data Breach to be contained, Mr. Cooper has not confirmed that the incident actually is contained or that the Data Breach has ended. And in fact, statements made to date indicate the incident is still ongoing. In its November 9, 2023 update to its security incident posting, Mr. Cooper said “we are working around the clock with cybersecurity experts to resolve this issue as soon as possible.”

⁵ Mr. Cooper Group, Nov. 2023 Form 8-K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/4edccf79-a641-4e5a-bf8c-0d681457778c.pdf>. This is the exact scenario contemplated in Mr. Cooper’s annual report: “We and others in our industry are regularly the subject of attempts by attackers to gain unauthorized access to our networks, systems, and data[.]” See Mr. Cooper Group 2022 Annual Report, https://s1.q4cdn.com/275823140/files/doc_financials/2022/ar/book-marked-annual-report-final.pdf.

unauthorized bank transactions they believe are directly tied to the Data Breach.

6. As a result of Mr. Cooper's failure to protect the sensitive information it was entrusted to safeguard, Plaintiffs and Class members have suffered harm and have been exposed to a significant and continuing risk of identity theft, financial fraud, and other identity-related fraud indefinitely.

PARTIES

7. Defendant Mr. Cooper Group Inc. is a Delaware corporation registered with the state of Texas with its principal place of business at 8950 Cypress Waters Blvd., Coppell, TX 75019.

8. Plaintiffs Jerold Short and Carlette Short are residents and citizens of Florida and have been customers of Mr. Cooper since 2022.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000, there are more than 100 proposed Class members, and minimal diversity exists because Mr. Cooper and at least one Class member are citizens of different States. This Court also has supplemental jurisdiction over the claims in this case pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy under Article III of the United States Constitution.

10. The Court has personal jurisdiction over Mr. Cooper because Mr. Cooper is headquartered in Coppell, Texas. Mr. Cooper also conducts substantial business in Texas related to Plaintiffs and Class members and has thereby established minimum contacts with Texas

sufficient to authorize this Court's exercise of jurisdiction over Mr. Cooper.

11. Venue in the Northern District of Texas is proper under 28 U.S.C. § 1391 because Mr. Cooper resides in this District, and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, including Mr. Cooper collecting and/or storing the PII of Plaintiffs and Class members.

FACTUAL ALLEGATIONS

Mr. Cooper's Privacy Practices

12. Mr. Cooper is a mortgage company that "provides servicing, origination and transaction-based services related to single family residences throughout the United States."⁶ Mr. Cooper holds itself out as "one of the largest home loan servicers and originators in the country focused on delivering a variety of servicing and lending products, services, and technologies."⁷

13. Mr. Cooper emphasizes its data security to potential customers, representing that "customer service, trust and confidence is a high priority. That's why we welcome this opportunity to describe our privacy policies, the steps we take to protect and maintain your information and to let you know how you can choose how your customer information may be shared."⁸

14. Aware of how important data security is to customers, Mr. Cooper's website accessible privacy policy represents to those customers: "Keeping financial information is one of our most important responsibilities. Only those persons who need it to perform their job responsibilities are authorized to access your information. We take commercially reasonable

⁶ Mr. Cooper Group, Oct. 2023 Form 10-Q, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/6ea7ec4e-5b61-47c1-b6d8-ba74e4ccd120.pdf> (last visited Nov. 20, 2023).

⁷ *Id.*

⁸ Mr. Cooper Group, Privacy Policy, <https://www.mrcooper.com/privacy> (last visited Nov. 20, 2023).

precautions to protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards.”⁹ In the same policy, Mr. Cooper represents that the same protections will apply to former Mr. Cooper customers.

15. In the course of providing services, Mr. Cooper collects customers’ highly sensitive PII and regularly stores and transfers such information as part of its regular business operations. According to Mr. Cooper’s privacy policy, this information includes “names, phone numbers, email addresses, mailing address, approximate location, technology habits (e.g. what browser you use, if you are using a tablet or mobile phone, and internet activity), and commercial information like the products/services you’ve purchased from us,” as well as social security numbers, employment history, and bank account numbers.¹⁰ Mr. Cooper claims to collect this information directly from customers, internet advertisers, mortgage lead generators, other mortgage servicers, government entities, and cookies or other online tools and technology.

16. Mr. Cooper collects this information for a variety of purposes including “making and servicing mortgage loans,” “performing services,” “providing financing and customer service,” “providing online products and services,” “marketing and advertising.” In Mr. Cooper’s own words, “You could say that we collect, process, store and disclose your information.”¹¹

17. In its 2022 Annual Report, Mr. Cooper acknowledged the role PII plays in its business operations: “As a part of conducting business, we receive, transmit and store a large

⁹ *Id.*

¹⁰ Mr. Cooper Group, California Consumer Privacy Act, <https://www.mrcooper.com/privacy/ccpa> (last visited Nov. 20, 2023).

¹¹ *Id.*

volume of personally identifiable information and other user data.”¹²

18. By obtaining, collecting, and storing the PII of Plaintiffs and Class members, Mr. Cooper assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosure. Plaintiffs and Class members relied on Mr. Cooper to keep their information confidential and secure.

19. Unfortunately, Mr. Cooper did not abide by its promises to keep customers’ PII secure.

The Data Breach

20. On or before October 31, 2023, an unauthorized party infiltrated Mr. Cooper’s network and accessed certain highly sensitive PII stored on its servers. Mr. Cooper has not yet disclosed what type of data was exposed. Although Mr. Cooper has not announced how many customers were impacted, it boasts of serving 4.3 million current customers and likely maintains information for millions of former customers as well.

21. Other than announcing it discovered the breach on October 31, 2023, and that the breach exposed customer data, Mr. Cooper has not provided any additional details of the breach or sent out breach notification letters to impacted victims.

22. All available evidence, however, suggests that the breach is massive in size and scope. On November 1, 2023, Mr. Cooper sent a communication to customers stating that “We are currently experiencing a technical outage that may delay your payment this month. Rest assured, you will not be charged any late fees or incur any penalties due to this issue. Once your payment

¹² Mr. Cooper Group 2022 Annual Report, https://s1.q4cdn.com/275823140/files/doc_financials/2022/ar/book-marked-annual-report-final.pdf (last visited Nov. 20, 2023).

is processed, you will receive a confirmation.”

23. On November 2, 2023, Mr. Cooper sent another communication stating that: “On October 31st, Mr. Cooper became the target of a cyber security incident and took immediate steps to lock down our systems in order to keep your data safe. We are working to resolve the issue as quickly as possible.” It provided a link to its website where it provided the following additional information:

As part of our ongoing investigation, we now believe that certain customer data was exposed. We are continuing to investigate precisely what information was exposed. In the coming weeks, we will mail notices to any affected customer and provide them with complimentary credit monitoring services.

Until that time, it is always advisable to monitor your financial accounts and credit reports for any unauthorized activity. You should immediately report any unusual activity to your financial institution. You can also contact the three major credit bureaus to place a “fraud alert” on your file at no cost, which alerts creditors to contact you before they open a new credit under your Social Security number. Additionally, you should update your passwords frequently and with increasing complexity, and be mindful to not use the same password across multiple personal accounts.

Once again, we apologize for any inconvenience or concern this situation may have caused.

24. This communication from Mr. Cooper has been repeatedly updated. As of November 10, 2023, Mr. Cooper claimed the impacted systems did not store customer financial information: “Please note that Mr. Cooper does not store banking information related to mortgage

payments on our systems. This information is hosted with a third-party provider and, based on the information we have to date, we do not believe it was affected by this incident.” On November 15, 2023, Mr. Cooper removed that language from its online notice, calling into question whether customer financial information *was* accessible from Mr. Cooper’s systems.¹³

25. Mr. Cooper’s securities filings provide only slightly more detail, stating that Mr. Cooper “initiated response protocols, including deploying containment measures to protect systems and data and shutting down certain systems as a precautionary measure.”¹⁴

26. Mr. Cooper’s notices raise more questions than they answered. For example, they do not state which of Mr. Cooper’s systems were impacted, how many customers were affected, what information was accessed, whether it was exfiltrated from Mr. Cooper’s systems, and whether the breach has actually been stopped.

27. Mr. Cooper’s lack of disclosure has likely prevented millions of current and former customers of Mr. Cooper from taking meaningful actions to protect themselves in the face of serious and imminent harm.

The Data Breach was Foreseeable and Preventable

28. In response to the Data Breach, Mr. Cooper stated it “lock[ed] down our systems”¹⁵ and “initiated a thorough investigation to determine the cause and full extent of the incident.”¹⁶

¹³ Mortgage Giant Mr. Cooper Says Customer Data Exposed in Breach, <https://www.bleepingcomputer.com/news/security/mortgage-giant-mr-cooper-says-customer-data-exposed-in-breach/> (last visited Nov. 20, 2023).

¹⁴ Mr. Cooper Group, Nov. 2023 Form 8-K, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/51b7c580-cebd-4fa6-8d5b-f22bb7da7c5f.pdf> (last visited Nov. 20, 2023).

¹⁵ Mr. Cooper Group, Notice of Cybersecurity Incident, <https://incident.mrcooperinfo.com/>

¹⁶ Mr. Cooper Group, Nov. 2023 Form 8-K/A, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/4edccf79-a641-4e5a-bf8c-0d681457778c.pdf>.

29. But Mr. Cooper, like any company of its size that stores massive amounts of sensitive PII, should have had robust protections in place to detect and terminate a successful intrusion long before access and exposure of customer data. Mr. Cooper's failure to prevent the breach is inexcusable given its knowledge that it was a prime target for cyberattacks.

30. In 2021, Bloomberg described the financial services industry as experiencing an "unrelenting year of fighting off cyber threats," and warned that financial services providers "should expect more of the same or even worse."¹⁷ As noted in the article, the Financial Services Information Sharing and Analysis Center's ("FS-ISAC") annual report on cyber threats predicted "current trends to continue and possibly worsen over the next year," stating cybersecurity is "no longer just a back-office cost." These increases are "due to several factors," including the "rapid digitization of financial services, which accelerated during the pandemic," and "increased entry points for cyber criminals to possibly exploit." Teresa Walsh, who leads FS-ISAC's global intelligence office, described the financial sector as experiencing "a dizzying number of vulnerabilities."

31. Mr. Cooper recognized this risk in its own regulatory filings. For example, in its 2022 Annual Report, Mr. Cooper acknowledged the business risk of suffering a cybersecurity incident:

Cybersecurity risks for the financial services industry have increased significantly in recent years due to new technologies, the reliance on technology to conduct financial transactions and the increased sophistication of organized crime and hackers. Those parties also may attempt to misrepresent personal or financial information to obtain loans or other financial products from us or attempt to fraudulently induce employees, customers, or other users of our systems to disclose confidential information in order to gain access to our data or that

¹⁷ *Financial Firms Brace for More Cyber Threats After Trying 2021*, BLOOMBERG, <https://www.bloomberg.com/news/articles/2022-03-10/financial-firms-poised-for-worse-cyber-threats-after-trying-year> (last visited Nov. 20, 2023)

of our customers.

We and others in our industry are regularly the subject of attempts by attackers to gain unauthorized access to our networks, systems, and data, or to obtain, change, or destroy confidential data (including personal identifying information of individuals) through a variety of means, including computer viruses, malware, phishing, ransomware and other attack vectors. These attacks may result in unauthorized individuals obtaining access to our confidential information or that of our customers, or otherwise accessing, damaging, or disrupting our systems or infrastructure.

A successful penetration or circumvention of the security of our or our vendors' systems or a defect in the integrity of our or our vendors' systems or cybersecurity could cause serious negative consequences for our business, including significant disruption of our operations, misappropriation of our confidential information or that of our customers, or damage to our computers or operating systems and to those of our customers and counterparties"¹⁸

32. Mr. Cooper also witnessed numerous high-profile cybersecurity incidents affecting other companies in the financial services sector, including credit reporting agency Equifax (147 million customers impacted, September 2017), Heartland Bank (130 million customers, January 2008), Capital One Bank (100 million customers, March 2019),¹⁹ JPMorgan Chase (83 million customers, October 2014), Experian (24 million customers, August 2020), First American Financial (885 million customers, May 2019), and Flagstar Bank (1.5 million customers, June 2022), among scores of others.

¹⁸Mr. Cooper Group 2022 Annual Report, https://s1.q4cdn.com/275823140/files/doc_financials/2022/ar/book-marked-annual-report-final.pdf (last visited Nov. 20, 2023).

¹⁹Capital One was assessed an \$80 million civil penalty by the Office of the Comptroller of the Currency ("OCC") due to its "failure to establish effective risk assessment processes prior to migrating significant information technology operations to the public cloud environment and the bank's failure to correct the deficiencies in a timely manner." OCC Assesses \$80 Million Civil Money Penalty Against Capital One, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Aug. 6, 2020), available at <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html> (last visited Nov. 20, 2023)

33. Consequently, Mr. Cooper knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including the significant costs that would be imposed on customers as a result of a breach.

34. But despite all of the publicly available knowledge of the continued compromises of PII and despite holding the PII of millions of customers, Mr. Cooper failed to use reasonable care in maintaining the privacy and security of the PII of Plaintiffs and Class members.

35. Had Mr. Cooper implemented industry standard security measures and adequately invested in data security, unauthorized parties likely would not have been able to access Mr. Cooper's systems and the Data Breach would have been prevented or much smaller in scope.

Value of PII

36. The PII of consumers remains of high value to criminals, as evidenced by the continued sale and trade of such information on underground markets found on the "dark web"—which is a part of the internet that is intentionally hidden and inaccessible through standard web browsers.

37. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁰ According to the Dark Web Price Index for 2021, payment card details for an account balance up to \$1,000 have an average market value of \$150, credit card details with an account balance up to \$5,000 have an average market value of \$240, stolen online banking logins with a minimum of \$100 on the account have an average market value of \$40, and

²⁰ Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Nov. 20, 2023).

stolen online banking logins with a minimum of \$2,000 on the account have an average market value of \$120.²¹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²² Other sources show sensitive private information selling for as much as \$363 per record.²³

38. Data sets that include PII demand a much higher price on the black market. For example, the information likely exposed in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.²⁴ The information likely disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

39. There is also an active and robust *legitimate* market for PII. In 2019, the data brokering industry alone was valued at \$200 billion.²⁵ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.²⁶ Consumers who agree to provide their web browsing history to the Nielsen Corporation can

²¹ Dark Web Price Index 2021, Zachary Ignoffo, June 10, 2023, available at: <https://www.privacyaffairs.com/dark-web-price-index-2021/>

²² In the Dark, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Nov. 20, 2023).

²³ Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

²⁴ See Jesse Damiani, *Your Social Security Number Costs \$4 on the Dark Web*, New Report Finds, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=770cee3a13f1> (last visited Nov. 20, 2023).

²⁵ David Lazarus, Column: Shadowy data brokers make the most of their invisibility cloak, Los Angeles Times (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

²⁶ <https://datacoup.com/#first-stop> (last visited Nov. 20, 2023).

receive up to \$50.00 a year.²⁷

40. Because their PII has independent value, Plaintiffs and Class members must take measures to protect it including by, as Mr. Cooper's online notice instructs, placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, and reviewing and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

ALLEGATIONS RELATING TO PLAINTIFFS

41. Plaintiffs Jerold and Carlette Short are residents and citizens of the State of Florida. Plaintiffs' mortgage was originated in 2017 and acquired by Mr. Cooper in 2022. In the course of obtaining their mortgage, Plaintiffs were required to provide their PII, including names, social security numbers, dates of birth, address, and highly sensitive bank account information.

42. Plaintiffs received notice from Mr. Cooper that its payment systems were down and later that Mr. Cooper had experienced a cyber security incident that was to blame. As a result, Plaintiffs were interrupted from making their regular mortgage payments.

43. Plaintiffs spent time and effort trying to research the breach but details from Mr. Cooper were scarce. Given their inability to make regular payments and Mr. Cooper's direction "to monitor your financial accounts and credit reports for any unauthorized activity", Plaintiffs could only assume the breach was serious and their PII was likely impacted.

44. To attempt to mitigate the risk of harm presented by the Data Breach, Plaintiffs spent time and effort researching the breach and reviewing their credit profiles and financial

²⁷Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited Nov. 20, 2023).

account statements for evidence of unauthorized activity, which they will continue to do indefinitely.

45. Plaintiffs have also suffered significant distress knowing their highly sensitive PII is no longer confidential and their financial account information is potentially compromised. Given the nature of the information likely exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiffs face a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

46. Because Mr. Cooper continues to store and share Plaintiffs' PII in the regular course of its business, Plaintiffs have a continuing interest in ensuring that the PII is protected and safeguarded from additional unauthorized access.

Mr. Cooper Failed to Comply with Federal Law and Regulatory Guidance

47. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (FTC) has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.²⁸

48. The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as

²⁸FTC, Start With Security, A Guide for Business, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Nov. 20, 2023).

a means to protect sensitive data.²⁹ Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.³⁰

49. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.³¹

50. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.³²

²⁹FTC, Protecting Personal Information: A Guide for Business, <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited Nov. 20, 2023).

³⁰*Id.*

³¹ FTC, Start With Security, A Guide for Business, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Nov. 20, 2023)

³²FTC, Privacy and Security Enforcement, <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Nov. 20, 2023)

51. Mr. Cooper was fully aware of its obligation to implement and use reasonable measures to protect customers' PII but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Mr. Cooper's failure to employ reasonable measures to protect against unauthorized access to customer information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. As a "financial institution,"³³ that collects nonpublic personal information,³⁴ Mr. Cooper also failed to comply with the Gramm-Leach-Bliley Act ("GLBA"),³⁵ which imposes "an affirmative and continuing obligation" on all financial institutions to "respect the privacy of [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. Consistent with that duty, financial institutions are required to establish appropriate safeguards "to insure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." *Id.*

53. Mr. Cooper also failed to comply with the Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b). The Safeguards Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable

³³ The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

³⁴ As defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n), and 12 C.F.R. § 1016.3(p)(1).

³⁵ 15 U.S.C. §§ 6801.1, *et seq.*

administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control these risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

54. Though limited detail is available on the Data Breach and how it occurred, Mr. Cooper's failure to safeguard its customers' PII suggests Mr. Cooper failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, encryption, and intrusion detection and prevention.

The Impact of the Data Breach on Victims

55. Mr. Cooper's failure to keep Plaintiffs' and Class members' PII secure has severe ramifications. Given the sensitive nature of the PII likely stolen in the Data Breach—names, date of birth, Social Security numbers, and potentially financial account information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class members now and into the indefinite future. Some customers have already reported experiencing fraud associated with their financial accounts utilized to make mortgage payments to Mr. Cooper.

56. As a result, Plaintiffs and Class members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

57. As discussed above, the PII likely exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."³⁶

58. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

59. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

60. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;

³⁶A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% report problems with family members as a result of the breach;
- 10% reported feeling suicidal.³⁷

61. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.³⁸

62. Plaintiffs and Class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less personal

³⁷2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces, https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Nov. 20, 2023).

³⁸Identity Theft: The Aftermath 2017, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Nov. 20, 2023).

information to organizations that suffered a data breach.³⁹

63. Likewise, the American Bankers Association, reporting on a global consumer survey regarding concerns about privacy and data security, noted that 29% of consumers would avoid using a company that had experienced a data breach, with 63% of consumers indicating they would avoid such a company for a period of time.⁴⁰

64. Plaintiffs and Class members are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

65. Plaintiffs and Class members have a direct interest in Mr. Cooper's promises and duties to protect their PII, *i.e.*, that Mr. Cooper *not increase* their risk of identity theft and fraud. Because Mr. Cooper failed to live up to its promises and duties in this respect, Plaintiffs and Class members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Mr. Cooper's wrongful conduct. Through this remedy, Plaintiffs seek to restore themselves and Class members as close to the same position as they would have occupied but for Mr. Cooper's wrongful conduct,

³⁹ Fireeye, Beyond the Bottom Line: The Real Cost of Data Breaches, https://web.archive.org/web/20220205174527/https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Nov. 20, 2023).

⁴⁰ Margaret Weir Westby and Lisa Wolf, What Compliance Needs to Know in the Event of A Security Breach, *Banking Journal*, (Sep. 9, 2019), <https://bankingjournal.aba.com/2019/09/what-compliance-needs-to-know-in-the-event-of-a-security-breach/> (last visited Nov. 20, 2023).

namely its failure to adequately protect Plaintiffs' and Class members' PII.

66. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- a. the unconsented, uncompensated disclosure of confidential information to a third party;
- b. losing the value of access to their PII permitted by Mr. Cooper;
- c. identity theft and fraud resulting from the theft of their PII;
- d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- e. anxiety, emotional distress, and loss of privacy;
- f. the present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach;
- g. unauthorized charges and loss of use of and access to their accounts;
- h. lowered credit scores resulting from credit inquiries following fraudulent activities;
- i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and
- j. the continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or many unauthorized third parties.

67. To date, Mr. Cooper has done little to provide Plaintiffs and Class members with relief for the damages they have suffered as a result of the Data Breach—Mr. Cooper has only claimed it will offer identity monitoring services, which places the burden squarely on *customers*

to enroll and monitor their accounts. Mr. Cooper has not yet offered any other relief or protection.

68. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per individual. Even if Mr. Cooper (belatedly) offers a free version for a year or two, Plaintiffs and class members will need such services for many years given the nature of information likely compromised. This is a future cost Plaintiffs and Class members would not need to bear but for Mr. Cooper's failure to safeguard their PII.

69. Plaintiffs and Class members have an interest in ensuring that their PII is secured and not subject to further theft because Mr. Cooper continues to hold their PII.

CLASS ACTION ALLEGATIONS

70. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following class:

All individuals residing in the United States whose PII was accessed as a result of the Data Breach announced by Mr. Cooper in or around November 2023 (the "Class").

71. Specifically excluded from the Class are Mr. Cooper and its officers, directors, or employees; any entity in which Mr. Cooper has a controlling interest; and any affiliate, legal representative, heir, or assign of Mr. Cooper. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

72. **Jurisdictional Amount.** As alleged herein, Plaintiffs seek damages on behalf of themselves and potentially millions of putative class members, satisfying the \$5 million jurisdictional requirement of 28 U.S.C. § 1332(d)(2).

73. **Ascertainability.** The members of the Class are readily identifiable and ascertainable. Mr. Cooper and/or its affiliates, among others, possess the information to identify

and contact Class members.

74. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all of them is impracticable. Mr. Cooper's statements reveal that the Class potentially contains over 4.3 million individuals whose PII was compromised in the Data Breach.

75. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of all Class members because they were customers of Mr. Cooper, impacted by the Data Breach, and suffered harm as a result.

76. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and their interests are aligned with Class members' interests. Plaintiffs were subject to the same Data Breach as Class members, suffered similar harms, and face similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including scores of data breach and privacy cases.

77. **Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class members. The common questions of law and fact include, without limitation:

- a. Whether Mr. Cooper owes Plaintiffs and Class members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

- b. Whether Mr. Cooper acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class members' PII;
- c. Whether Mr. Cooper violated its duty to implement reasonable security systems to protect Plaintiffs' and Class members' PII;
- d. Whether Mr. Cooper's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class members;
- e. Whether Mr. Cooper provided timely notice of the Data Breach to Plaintiffs and Class members; and
- f. Whether Plaintiffs and Class members are entitled to compensatory damages, punitive damages, and/or nominal damages as a result of the Data Breach.

78. Mr. Cooper has engaged in a common course of conduct and Plaintiffs and Class members have been similarly impacted by Mr. Cooper's failure to maintain reasonable security procedures and practices to protect customers' PII.

79. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF ON BEHALF OF THE CLASS

COUNT I
BREACH OF CONTRACT

80. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

81. Mr. Cooper's Privacy Policy is an agreement between Mr. Cooper and individuals who provided their PII to Mr. Cooper, including Plaintiffs and Class members.

82. Mr. Cooper represents that its Privacy Policy applies to information it collects about individuals who seek, apply for, or obtain Mr. Cooper's financial products and services.

83. Mr. Cooper's Privacy Notice stated at the time of the Data Breach that Mr. Cooper "use[s] security measures that comply with federal law," and "[t]hese measures include computer safeguards and secured files and buildings," in order to "protect your personal information from unauthorized access and use."

84. Mr. Cooper further agreed at the time of the Data Breach that it would only share data under certain enumerated circumstances, which include: "[f]or our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus," "[f]or our marketing purposes – to offer our products and services to you," "[f]or joint marketing with other financial companies," and "[f]or our affiliates' everyday business purposes – information about your transactions and experiences."

85. None of the enumerated circumstances involve sharing Plaintiffs or the Class members' PII with unauthorized parties.

86. Plaintiffs and Class members, on the one side, and Mr. Cooper, on the other, formed a contract when Plaintiffs and Class members obtained services from Mr. Cooper, or otherwise transmitted or authorized the transmission of PII to Mr. Cooper subject to its Privacy Policy.

87. Plaintiffs and Class members fully performed their obligations under the contracts with Mr. Cooper.

88. Mr. Cooper breached its agreement with Plaintiffs and Class members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

89. As a direct and proximate result of Mr. Cooper's breach of contract, Plaintiffs and Class members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT

90. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs and assert this claim in the alternative to their breach of contract claim to the extent necessary.

91. Mr. Cooper acquired and maintained the PII of Plaintiffs and the Class that it received either directly or indirectly from other mortgage originators.

92. When Plaintiffs and Class members paid money and provided their PII to their mortgage originators, either directly or indirectly, in exchange for services, they entered into implied contracts with their mortgage originators and their business associates, including Mr. Cooper.

93. As part of these transactions, Mr. Cooper agreed to safeguard and protect the PII of Plaintiffs and Class members. Implicit in the transactions between Mr. Cooper and Class members was the obligation that Mr. Cooper would utilize reasonable measures to keep the PII secure; Mr.

Cooper would limit access to PII; Mr. Cooper would use the PII for approved business purposes only; and Mr. Cooper would retain PII only as necessary to perform necessary business functions.

94. Additionally, Mr. Cooper implicitly promised to retain this Plaintiffs' and Class members' PII only under conditions that kept such information secure and confidential.

95. Plaintiffs and Class members believed that Mr. Cooper would use part of the monies paid directly or indirectly to Mr. Cooper under the implied contracts to fund adequate and reasonable data security practices to protect their PII.

96. Plaintiffs and Class members would not have provided and entrusted their PII to Mr. Cooper or would have paid less for Mr. Cooper's services in the absence of the implied contract between them and Mr. Cooper. The safeguarding of Plaintiffs' and Class members' PII was critical to realizing the intent of the parties.

97. Mr. Cooper breached its implied contract with Plaintiffs and Class members by failing to reasonably safeguard and protect their PII, which was compromised as a result of the Data Breach.

98. As a direct and proximate result of Mr. Cooper's breach of implied contract, Plaintiffs and Class members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT III **NEGLIGENCE**

99. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

100. Upon accepting transmission of Plaintiffs and Class members' PII, Mr. Cooper owed a duty of reasonable care in handling and using this information and securing and protecting

the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Mr. Cooper was required to design, maintain, and test its security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Plaintiffs and the Class members. Mr. Cooper further owed to Plaintiffs and the Class members a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

101. Mr. Cooper's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Mr. Cooper and its customers, which is recognized by laws and regulations including but not limited to the FTC Act, the GLBA, and common law.

102. Mr. Cooper owed this duty to Plaintiffs and Class members because Mr. Cooper collected their PII in the course of its business and it was reasonably foreseeable that Plaintiffs and Class members would be harmed if Mr. Cooper failed to keep their PII secure.

103. Mr. Cooper owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, to design, implement, and monitor data security systems, policies, and processes to protect against foreseeable threats, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected customers' PII.

104. The imposition of a duty of care on Mr. Cooper to safeguard the PII they maintained is appropriate because any social utility of Mr. Cooper's conduct is outweighed by the injuries suffered by Plaintiffs and Class members as a result of the Data Breach.

105. Mr. Cooper breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs and Class members' PII, as alleged and discussed above.

106. It was foreseeable that Mr. Cooper's failure to use reasonable measures to protect Class members' PII would result in injury to Plaintiffs and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

107. As a direct and proximate result of Mr. Cooper's negligence, Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach, including, but not limited to: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (viii) the present value of ongoing credit monitoring and identity defense services necessitated by Mr. Cooper's Data Breach; and (ix) any nominal damages that may be awarded.

COUNT IV
NEGLIGENCE *PER SE*

108. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

109. Pursuant to Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Mr. Cooper had a duty to provide fair and adequate computer systems and data security practices to

safeguard Plaintiffs' and Class members' PII.

110. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Mr. Cooper, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

111. Mr. Cooper violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Mr. Cooper's conduct was unreasonable given the nature and amount of PII it obtained, stored, and disseminated in the regular course of its business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class members if their PII was exposed.

112. The harms that occurred as a result of the Data Breach are the types of harms the FTC Act was intended to protect against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harms as those suffered by Plaintiffs and Class members here.

113. Mr. Cooper likewise violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by, among other things: (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's internal systems that were inadequately secured; (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system; (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information; (d) failing to adequately (i) test and/or monitor the system were the Data Breach occurred and (ii) update

and/or further secure its data security practices in light of the heightened risk environment; and (e) failing to send opt-out notices and afford a reasonable opportunity to opt out of disclosures before sharing the PII of millions individuals with one or more non-affiliated third parties.

114. Mr. Cooper's violations of Section 5 of the FTC Act and the GLBA constitutes negligence *per se*.

115. Plaintiffs and Class members are within the class of persons these federal laws were designed intended to protect.

116. Mr. Cooper knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location, Mr. Cooper's vulnerability to network attacks, and the importance of adequate security.

117. Mr. Cooper breached its duty to Plaintiffs and Class members in numerous ways, as described herein, including by:

- a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiffs and Class members;
- b. Failing to comply with industry standard data security measures leading up to the Data Breach;
- c. Failing to comply with its own Privacy Policy;
- d. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;
- e. Failing to adequately monitor, evaluate, and ensure the security of Mr. Cooper's network and systems;
- f. Failing to recognize in a timely manner that PII had been compromised; and
- g. Failing to timely and adequately disclose the Data Breach.

118. Plaintiffs' and Class members' PII would not have been compromised but for Mr.

Cooper's wrongful and negligent breach of its duties.

119. Mr. Cooper's failure to take proper security measures to protect the sensitive PII of Plaintiffs and Class members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII by unauthorized third parties. Given that financial service providers are prime targets for hackers, Plaintiffs and Class members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by Mr. Cooper.

120. It was also foreseeable that Mr. Cooper's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiffs and Class members.

121. As a direct and proximate result of Mr. Cooper's negligence *per se*, Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach, including but not limited to: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (viii) the present value of ongoing credit monitoring and identity defense services

necessitated by Mr. Cooper's Data Breach; and (ix) any nominal damages that may be awarded.

COUNT V
UNJUST ENRICHMENT

122. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs and assert this claim in the alternative to their breach of contract claims to the extent necessary.

123. Plaintiffs and Class members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, used by, and maintained by Mr. Cooper and that was ultimately stolen in the Mr. Cooper Data Breach.

124. Mr. Cooper benefited by the conferral upon it of the PII pertaining to Plaintiffs and the Class members and by its ability to retain, use, and profit from that information. Mr. Cooper understood and valued this benefit.

125. Mr. Cooper also understood and appreciated that the PII pertaining to Plaintiffs and Class members was private and confidential and its value depended upon Mr. Cooper maintaining the privacy and confidentiality of that PII.

126. Without Mr. Cooper's willingness and commitment to maintain the privacy and confidentiality of the PII, that PII would not have been transferred to and entrusted to Mr. Cooper. Further, if Mr. Cooper had disclosed that its data security measures were inadequate, it would not have been permitted to continue in operation by regulators or its customers.

127. Mr. Cooper admits that it uses the PII it collects for, among other things: "marketing and promotional communications."

128. Mr. Cooper was unjustly enriched by profiting from the use of Plaintiffs' and Class members' PII as well as the services and products it was able to market, sell, and create under the false pretense it had adequate systems in place to protect customers' PII to the detriment of

Plaintiffs and the Class members.

129. Mr. Cooper also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class members' PII and profits it gained through the use of Plaintiffs' and Class members' PII.

130. As a result of Mr. Cooper's wrongful conduct, Mr. Cooper has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class members.

131. It is inequitable, unfair, and unjust for Mr. Cooper to retain these wrongfully obtained benefits. Mr. Cooper's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

132. Plaintiffs and Class members have no adequate remedy at law.

133. Mr. Cooper is therefore liable to Plaintiffs and Class members for restitution or disgorgement in the amount of the benefit conferred on Mr. Cooper as a result of its wrongful conduct, including specifically: the value to Mr. Cooper of the PII that was stolen in the Data Breach; the profits Mr. Cooper received and is receiving from the use of that information; the amounts that Mr. Cooper overcharged Plaintiffs and Class members for use of Mr. Cooper's products and services; and the amounts that Mr. Cooper should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class members' PII.

COUNT VI
INVASION OF PRIVACY

134. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

135. Plaintiffs and Class members shared PII with Mr. Cooper and/or its affiliates that Plaintiffs and Class members wanted to remain private and non-public.

136. Plaintiffs and Class members reasonably expected that the PII they shared with Mr.

Cooper would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose.

137. Mr. Cooper intentionally intruded into Plaintiffs' and Class members' seclusion by disclosing without permission their PII to a criminal third party.

138. By failing to keep Plaintiffs' and Class members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Mr. Cooper unlawfully invaded Plaintiffs' and Class members' privacy right to seclusion by, *inter alia*:

- a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;
- b. Invading their privacy by improperly using their PII properly obtained for another purpose, or disclosing it to unauthorized persons;
- c. Failing to adequately secure their PII from disclosure to unauthorized persons; and
- d. Enabling the disclosures of their PII without consent.

139. Plaintiffs' and Class members' PII that was compromised during the Data Breach was highly sensitive, private, and confidential, as it likely included Social Security numbers and other information that is the type of sensitive, personal information that one normally expects will be protected from exposure by the entity charged with safeguarding it.

140. Mr. Cooper's intrusions into Plaintiffs' and Class members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

141. As a direct and proximate result of Mr. Cooper's invasion of privacy, Plaintiffs and Class members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT VII
BREACH OF CONFIDENCE

142. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

143. Plaintiffs and Class members maintained a confidential relationship with Mr. Cooper whereby Mr. Cooper undertook a duty not to disclose PII provided by Plaintiffs and Class members to unauthorized third parties. Such PII was confidential, novel, highly personal and sensitive, and not generally known.

144. Mr. Cooper knew Plaintiffs' and Class members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII it collected, stored, and maintained.

145. Plaintiffs' and Class members' PII was disclosed to unauthorized parties in violation of this understanding. The disclosure occurred because Mr. Cooper failed to implement and maintain reasonable safeguards to protect its customers' PII and failed to comply with industry-standard data security practices.

146. Plaintiffs and Class members suffered harm the moment an unconsented disclosure of their confidential information to an unauthorized third party occurred.

147. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT VIII
DECLARATORY AND INJUNCTIVE RELIEF

148. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

149. Plaintiffs and the Class pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

150. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint. An actual controversy has arisen in the wake of the Data Breach regarding Mr. Cooper's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Mr. Cooper is currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their PII. Plaintiffs and the Class remain at imminent risk that further compromises of their PII will occur in the future.

151. The Court should also issue prospective injunctive relief requiring Mr. Cooper to employ adequate security practices consistent with law and industry standards to protect employee and patient PII.

152. Mr. Cooper still possesses the PII of Plaintiffs and the Class.

153. To Plaintiffs' knowledge, Mr. Cooper has made no announcement that it has changed its data storage or security practices relating to the PII.

154. To Plaintiffs' knowledge, Mr. Cooper has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

155. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Mr. Cooper. The risk of

another such breach is real, immediate, and substantial.

156. As described above, actual harm has arisen in the wake of the Data Breach regarding Mr. Cooper's contractual obligations and duties of care to provide security measures to Plaintiffs and Class members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their PII and Mr. Cooper's failure to address the security failings that led to such exposure.

157. There is no reason to believe that Mr. Cooper's employee training and security measures are any more adequate now than they were before the Data Breach to meet Mr. Cooper's contractual obligations and legal duties.

158. The hardship to Plaintiffs and Class members if an injunction is not issued exceeds the hardship to Mr. Cooper if an injunction is issued. Among other things, if another data breach occurs at Mr. Cooper, Plaintiffs and Class members will likely continue to be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Mr. Cooper of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Mr. Cooper has a pre-existing legal obligation to employ such measures.

159. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Mr. Cooper, thus eliminating the additional injuries that would result to Plaintiffs and the Class.

160. Plaintiffs and Class members therefore, seek a declaration (1) that Mr. Cooper's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Mr. Cooper must implement and maintain reasonable security measures, including, but

not limited to, the following:

- a. Ordering that Mr. Cooper engage internal security personnel to conduct testing, including audits on Mr. Cooper's systems, on a periodic basis, and ordering Mr. Cooper to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Mr. Cooper engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Mr. Cooper audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;
- d. Ordering that Mr. Cooper purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for its provision of services;
- e. Ordering that Mr. Cooper conduct regular database scanning and security checks; and
- f. Ordering that Mr. Cooper routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and those similarly situated, respectfully request the following relief:

- A. That the Court certify this action as a class action and appoint Plaintiffs and their Counsel to represent the Class;
- B. That the Court grant permanent injunctive relief to prohibit and prevent Mr. Cooper from continuing to engage in the unlawful acts, omissions, and practices described herein;
- C. That the Court award Plaintiffs and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Mr. Cooper as a result of their unlawful acts, omissions, and practices;

E. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses allowed by law; and

F. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

DATED: November 22, 2023

Respectfully Submitted,

/s/ Sara Hollan Chelette

Sara Hollan Chelette

Texas Bar No. 24046091

schelette@lynnllp.com

Christopher W. Patton

Texas Bar No. 24083634

cpatton@lynnllp.com

LYNN PINKER HURST & SCHWEGMANN LLP

2100 Ross Avenue, Suite 2700

Dallas, Texas 75201

Telephone: (214) 981-3800

Facsimile: (214) 981-3839

/s/ Norman E. Siegel

Norman E. Siegel* (Missouri Bar No. 44378)

J. Austin Moore* (Missouri Bar No. 64040)

Tanner J. Edwards* (Missouri Bar No 68039)

STUEVE SIEGEL HANSON LLP

460 Nichols Road, Suite 200

Kansas City, Missouri 64112

Telephone: (816) 714-7100

siegel@stuevesiegel.com

moore@stuevesiegel.com

tanner@stuevesiegel.com

Counsel for Plaintiffs and the Proposed Class

**** Pro Hac Vice Applications Forthcoming***